

Enumerating Network Hosts



Ricardo Reimao, OSCP, CISSP
Cybersecurity Consultant



Mapping your next targets



Module Overview



Understand the main network enumeration techniques

Implement a host discovery script

Implement a port scan script

Use PowerShell to find SMB shares



Course Scenario: Globomantics Red Team



Network Enumeration Techniques

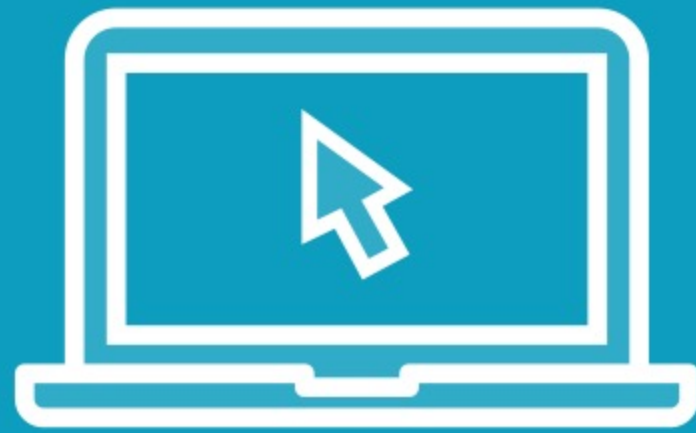
Host Discovery: Ping Scans

Port Scans: TCP-connect probing

SMB Scans: Using WMI and Net List



Demo



Finding live hosts on a network

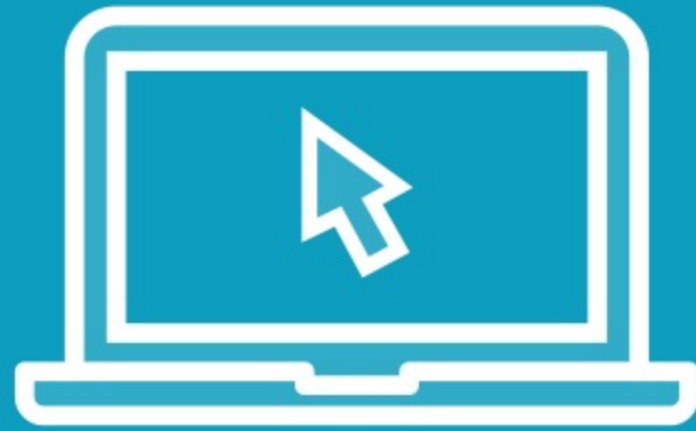
- Using ping scans



Course Scenario: Globomantics Red Team



Demo



Scanning open ports in hosts

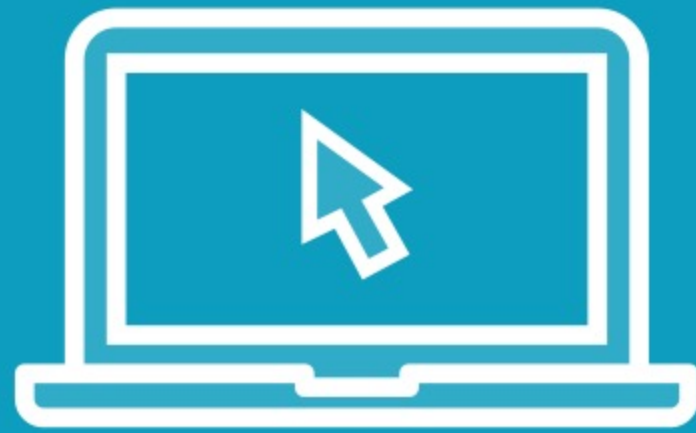
- Using TCP-Connect attempts



Course Scenario: Globomantics Red Team



Demo



Enumerating SMB shares

- Using WMI queries
- Using Net List



Course Scenario: Globomantics Red Team



Summary



The main techniques for network and port enumeration

How to create a ping scanner

How to create a port scanner

Enumerating SMB shares



Next up:
Active Directory Reconnaissance

